

John C. Bohren (California Bar No. 295292)
YANNI LAW APC
P.O. Box 12174
San Diego, CA 92112
Telephone: (619) 433-2803
Fax: (800) 867-6779
yanni@bohrenlaw.com

-AND-

Paul J. Doolittle (*Pro Hac Vice* Forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

Attorneys for Plaintiff

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA**

**KRYSTAL VARGHA, individually and on
behalf of all others similarly situated,**

Plaintiff,

v.

**POWERSCHOOL HOLDINGS, INC.,
D/B/A POWERSCHOOL,**

Defendant.

Case No.:

- 1. Negligence/Wantonness**
- 2. Breach of Implied Contract**
- 3. Unjust Enrichment**
- 4. Invasion of Privacy**
- 5. Violation of California's Unfair
Competition Laws ("UCL"); California
Business & Professions Code Sections
17200, *et seq.***

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

1 Plaintiff Krystal Vargha, (“Plaintiff”) brings this Class Action Complaint against
2 PowerSchool Holdings Inc., doing business as PowerSchool (“Defendant”) as an individual and on
3 behalf of all others similarly situated, and alleges, upon personal knowledge as to Plaintiff’s own
4 actions and to counsels’ investigation, and upon information and belief as to all other matters, as
5 follows:
6

7 **FACTUAL ALLEGATIONS**

8 1. Defendant PowerSchool is the largest provider of cloud-based education software
9 for K-12 education in the United States. Defendant’s software is used to support over 50 million
10 students in the United States.

11 2. While providing an education related service, Defendant collects, creates, or shares
12 information that can be used to identify an individual student, teacher, parent, or guardian.

13 3. Under the Family Educational Rights and Privacy Act (FERPA) of 1974, as
14 amended, enacted as section 444 of the General Education Provisions Act, Defendant is a
15 contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced
16 institutional services or functions. As such, Defendant was required not to disclose educational
17 records and personal data without the prior consent of the parent or eligible student.
18

19 4. Plaintiff brings this class action against Defendant for its unauthorized disclosure of
20 and failure to properly secure the personally identifiable information (“PII”) of numerous students,
21 teachers, parents and guardians, including, but not limited to: names, addresses, phone numbers,
22 emails, Social Security numbers, medical information, and academic information.
23

24 5. On or about, December 28, 2024, Defendant *become aware of a cybersecurity*
25 *incident involving* an unauthorized party using a compromised credential to gain access to
26 “PowerSource,” its customer support portal, which allowed further unauthorized access to, and
27
28

1 acquisition of, certain personal information stored within Defendant’s Student Information System
2 (SIS) (hereafter, the “Data Breach”).

3 6. On or about, January 9, 2025, the Charleston County School District sent an email
4 to Plaintiff notifying her of the cybersecurity incident involving Defendant and that her PII was
5 compromised in the Data Breach. Omitted from that notice was the details of the root cause of the
6 Data Breach, the specific types of data involved, the vulnerabilities exploited, and the remedial
7 measures undertaken to ensure such a breach does not occur again.

9 7. Defendant’s “Privacy Principles” provides, in relevant part, “We seek to protect our
10 customers’ personal data from unauthorized access, use, modification, disclosure, loss, or theft by
11 leveraging various reasonable security measures and methods to secure our customers’ personal
12 data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure
13 the confidentiality, integrity, and availability of our customers’ personal data by leveraging
14 technical, organizational, and where appropriate, physical security methods. Security protection at
15 PowerSchool is a cross-functional activity that intersects our workforce duties, and we have
16 relevant security and privacy policies to drive expectations from the workforce.”¹

18 8. Under Defendant’s “Accountability” principle, Defendant states: “For all of the
19 Privacy Principles stated above, PowerSchool endeavors to demonstrate compliance with each of
20 these principles. In additional internal audits, we have sought and obtained various privacy
21 program certifications to demonstrate accountability for these principles.”²

23 9. Under Defendant’s “Global Privacy Statement,” last updated October 1, 2024,
24 Defendant states, “Whether PowerSchool is a collector or processor of your data, PowerSchool is
25 committed to protecting your personal information. PowerSchool uses commercially reasonable
26

27 ¹ <https://www.powerschool.com/privacy>, last accessed January 9, 2025.

28 ² *Id.*

1 physical, administrative, and technical safeguards to preserve the confidentiality, integrity, and
2 availability of your personal information. Our systems are *regularly certified by third parties*
3 *against industry security standards* from AIPCA and ISO.”³

4
5 10. The Data Breach was a direct result of Defendant’s failure to implement reasonable
6 safeguards to protect PII from a foreseeable and preventable risk of unauthorized disclosure. Had
7 Defendant implemented administrative, technical, and physical controls consistent with industry
8 standards and best practices, it could have prevented the Data Breach.

9
10 11. Upon information and belief, the mechanism of the cyberattack and potential for
11 improper disclosure of Plaintiff’s data was a known risk to Defendant, and thus, Defendant was on
12 notice that failing to take steps necessary to secure the information from those risks left the data in
13 a dangerous condition.

14
15 12. More specifically, the risk of compromised credentials being used to gain
16 unauthorized access to PII was a known risk to Defendant. Under ISO/IEC 27001, for example,
17 Defendant could and should have implemented administrative and technical safeguards including,
18 but not limited to, the following:

- 19 a. Implement a password policy that: (i) required “strong passwords” or passwords
20 that are difficult for an attacker to guess; (ii) required passwords to be changed
21 frequently; (iii) uses account lockout to disable the account after a set number of
22 failed login attempts; (iv) ensured password history was tracked to prevent users
23 from reusing or repeating old passwords; and, (v) prohibited the same passwords
24 from being used across distinct services and systems.
- 25 b. Affected or compromised authentication information is changed immediately
26 upon notification of or any other indication of compromise.
- 27 c. Implement password restrictions in conjunction with other authentication
28 factors such as tokens, biometrics, keys or use Single Sign On (SSO) to reduce
the risk of passwords being compromised by attackers.
- d. Enforce password changes upon termination or change of employment when a
user has shared identities that remain active.

³ <https://www.powerschool.com/privacy>, last accessed January 9, 2025.

- e. Procedures should be established to verify the identity of a user prior to providing new, replacement or temporary passwords.
- f. After new systems and software programs are installed, change the default password immediately.
- g. Implement policies and procedures that, based upon the Defendant's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
- h. Implement a security awareness and training program for all members of Defendant's workforce, including procedures for guarding against, detecting, and reporting malicious software, unauthorized activity, and credential abuse.

13. Defendant's conduct resulted in the unauthorized disclosure of Plaintiff's private information to cybercriminals. The unauthorized disclosure of Plaintiff's PII constitutes an invasion of a legally protected privacy interest, that is traceable to the Defendant's failure to adequately secure the PII in its custody, and has resulted in actual, particularized, and concrete harm to the Plaintiff.

14. More specifically, since there were very few details in the notice regarding the Data Breach, Plaintiff and Class Members (later defined) were caused to: (i) spend money on mitigation measures like credit monitoring services, identity theft protection, and/or dark web searches; (ii) lose time and effort spent responding to the Data Breach; and/or (iii) experience emotional distress associated with reviewing accounts for fraud, changing usernames and passwords or closing accounts to prevent fraud, and general anxiety over the consequences of the Data Breach. The harm Plaintiff suffered can be redressed by a favorable decision in this matter.

15. Plaintiff faces a substantial risk of spam, phishing, or other social engineering attacks where their full names, addresses, email addresses, and phone numbers were stolen by a cybercriminal. Names, telephone numbers and email addresses can be used by cybercriminals to launch social engineering attacks designed to trick individuals into giving away sensitive information. Plaintiff may reasonably incur out of pocket costs for purchasing products to protect

1 from phishing, smishing (SMS message), vishing (voice messaging), pretexting, and other social
2 engineering-based attacks.

3 16. Plaintiff brings this class action lawsuit individually, and on behalf of all those
4 similarly situated, to address Defendant's inadequate data protection practices and for failing to
5 provide timely and adequate notice of the Data Breach.
6

7 17. Through this Complaint, Plaintiff seeks to remedy these harms individually, and on
8 behalf of all similarly situated individuals whose PII was accessed during the Data Breach.

9 18. Plaintiff has a continuing interest in ensuring that personal information is kept
10 confidential and protected from disclosure, and Plaintiff should be entitled to injunctive and other
11 equitable relief.
12

13 **JURISDICTION & VENUE**

14 19. This Court has subject matter jurisdiction over this action pursuant to the Class
15 Action Fairness Act ("CAFA"), 28 U.S.C. §1332, because this is a class action wherein the amount
16 in controversy exceeds the sum or value of \$5,000,000.00, exclusive of interest and costs, there are
17 more than 100 members in the proposed class, and at least one member of the class is a citizen of
18 a state different from each Defendant.

19 20. This Court has personal jurisdiction over Defendant because its principal place of
20 business is in this District. Defendant has also purposefully availed itself of the laws, rights, and
21 benefits of the State of California.
22

23 21. Venue is proper under 28 U.S.C. §1391(b) because Defendant maintains a principal
24 place of business in this District and a substantial part of the events and omissions giving rise to
25 Plaintiff's claims occurred in and emanated from this District.
26

27 **PARTIES**

28

22. Plaintiff Krystal Vargha is a resident citizen of Charleston County, South Carolina. Plaintiff is/was the parent or guardian of a minor-student in the Charleston County School District.

23. Defendant, PowerSchool Holdings, Incorporated, is a Delaware formed corporation that maintains a principal place of business at 150 Parkshore Drive, Folsom, Sacramento County, California 95630.

CLASS ALLEGATIONS

24. Plaintiff brings this nationwide class action individually, and on behalf of all similarly situated individuals, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

25. The Class that Plaintiff seeks to represent is defined as follows:

Nationwide Class

All individuals residing in the United States whose PII was accessed and acquired by an unauthorized party as a result of a data breach that occurred on, or about December 28, 2024, as reported to the Charleston County School District by Defendant (the “Class”).

South Carolina Subclass

All individuals residing in South Carolina whose PII was accessed and acquired by an unauthorized party as a result of the data breach that occurred on, or about December 28, 2024, as reported to the Charleston County School District by Defendant (the “South Carolina Subclass”).

26. Collectively, the Class and South Carolina Subclass are referred to as the “Classes” or “Class Members.”

27. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

1 28. Plaintiff reserves the right to amend the definitions of the Classes or add a Class or
2 Subclass if further information and discovery indicate that the definitions of the Classes should be
3 narrowed, expanded, or otherwise modified.

4 29. Numerosity: The members of the Classes are so numerous that joinder of all
5 members is impracticable, if not completely impossible. The exact number of Class Members is
6 unknown to Plaintiff at this time and such number is exclusively in the possession of Defendant,
7 upon information and belief, millions of individuals were impacted in Data Breach.

8 30. Common questions of law and fact exist as to all members of the Classes and
9 predominate over any questions affecting solely individual members of the Classes. The questions
10 of law and fact common to the Classes that predominate over questions which may affect individual
11 Class Members, includes the following:
12

- 13 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and
14 Class Members;
- 15 b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members
16 to unauthorized third parties;
- 17 c. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class
18 Members;
- 19 d. Whether Defendant required its third-party vendors to adequately safeguard the PII
20 of Plaintiff and Class Members;
- 21 e. When Defendant actually learned of the Data Breach;
- 22 f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and
23 Class Members that their PII had been compromised;
- 24 g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class
25 Members that their PII had been compromised;
- 26 h. Whether Defendant failed to implement and maintain reasonable security
27 procedures and practices appropriate to the nature and scope of the information
28 compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the practices, procedures, or
 vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory
 damages, and/or nominal damages as a result of Defendant's wrongful conduct;

1 k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the
2 imminent and ongoing harm faced as a result of the Data Breach.

3 31. Typicality: Plaintiff's claims are typical of those of the other members of the Classes
4 because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and
5 now suffers from the same violations of the law as each other member of the Classes.

6 32. Policies Generally Applicable to the Class: This class action is also appropriate for
7 certification because Defendant acted or refused to act on grounds generally applicable to the
8 Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards
9 of conduct toward the Class Members and making final injunctive relief appropriate with respect
10 to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members
11 uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect
12 to the Classes as a whole, not on facts or law applicable only to Plaintiff.

13 33. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of
14 the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic
15 to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the
16 Class Members and the infringement of the rights and the damages suffered are typical of other
17 Class Members. Plaintiff has retained counsel experienced in complex class action and data breach
18 litigation, and Plaintiff intends to prosecute this action vigorously.

19 34. Superiority and Manageability: The class litigation is an appropriate method for fair
20 and efficient adjudication of the claims involved. Class action treatment is superior to all other
21 available methods for the fair and efficient adjudication of the controversy alleged herein; it will
22 permit a large number of Class Members to prosecute their common claims in a single forum
23 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and
24 expense that hundreds of individual actions would require. Class action treatment will permit the
25 adjudication of relatively modest claims by certain Class Members, who could not individually
26
27
28

1 afford to litigate a complex claim against large corporations, like Defendant. Further, even for those
2 Class Members who could afford to litigate such a claim, it would still be economically impractical
3 and impose a burden on the courts.

4 35. The nature of this action and the nature of laws available to Plaintiff and Class
5 Members make the use of the class action device a particularly efficient and appropriate procedure
6 to afford relief for the wrongs alleged because Defendant would necessarily gain an unconscionable
7 advantage since Defendant would be able to exploit and overwhelm the limited resources of each
8 individual Class Member with superior financial and legal resources; the costs of individual suits
9 could unreasonably consume the amounts that would be recovered; proof of a common course of
10 conduct to which Plaintiff was exposed is representative of that experienced by the Classes and will
11 establish the right of each Class Member to recover on the cause of action alleged; and individual
12 actions would create a risk of inconsistent results and would be unnecessary and duplicative of this
13 litigation.

14 36. The litigation of the claims brought herein is manageable. Defendant's uniform
15 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
16 Members demonstrates that there would be no significant manageability problems with prosecuting
17 this lawsuit as a class action.

18 37. Adequate notice can be given to Class Members directly using information
19 maintained in Defendant's records.

20 38. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
21 properly secure the PII of Classes, Defendant may continue to refuse to provide proper notification
22 to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set
23 forth in this Complaint.
24
25
26
27
28

39. Further, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

40. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiff and the Classes of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, sharing, storing, and safeguarding their PII;
- c. Whether Defendant's (or their vendors') security measures to protect its network were reasonable in light of industry best practices;
- d. Whether Defendant's (or their vendors') failure to institute adequate password management, authentication, and other safeguards amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII;
- f. Whether Defendant made false representations about their data privacy practices and commitment to the security and confidentiality of personal information; and
- g. Whether adherence to industry standards and data protection best practices would have prevented the Data Breach.

CAUSES OF ACTION
(On behalf of Plaintiff and the Classes)

COUNT 1: NEGLIGENCE/WANTONNESS

41. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

42. Defendant collects and receives various educational records and other PII, regarding students, teachers, parents and guardians, including Plaintiff and Class Members, in the ordinary course of providing education related products or services.

1 43. Defendant had full knowledge of the types of PII it collected and the types of harm
2 that Plaintiff and Class Members would suffer if that data was accessed and exfiltrated by an
3 unauthorized third-party.

4 44. Under FERPA Defendant had a duty not to disclose educational records without the
5 prior consent of the parent or eligible student. Defendant permitted its information technology
6 environment to remain vulnerable to foreseeable threats, which created an atmosphere for the Data
7 Breach to occur. Despite knowledge of the substantial risk of harm created by these conditions,
8 Defendant consciously disregarded the risk, thus permitting the Data Breach to occur.

9 45. By collecting, storing, sharing, and using the Plaintiff's and Class Members' PII for
10 commercial gain, Defendant assumed a duty to use reasonable means to safeguard the personal data
11 it obtained.

12 46. Defendant's duty included a responsibility to ensure it: (i) implemented reasonable
13 administrative, technical, and physical measures to detect and prevent unauthorized intrusions into
14 its information technology and/or cloud environments; (ii) contractually obligated its vendors to
15 adhere to the requirements of Defendant's privacy policy; (iii) complied with applicable statutes
16 and data protection obligations; (iv) provided timely notice to individuals impacted by a data
17 breach; and, (v) exercised appropriate clearinghouse practices to remove PII that Defendant was no
18 longer required to retain.

19 47. Defendant had a duty to notify Plaintiff and the Classes of the Data Breach promptly
20 and adequately. Such notice was necessary to allow Plaintiff and the Classes to take steps to
21 prevent, mitigate, and repair any fraudulent usage of their PII.

22 48. Defendant breached its duties, and thus was negligent, by failing to use reasonable
23 measures to protect Class Members' PII. The specific negligent acts and omissions committed by
24 Defendant includes, but are not limited to, the following:

- a) Failing to implement reasonable password management and user authentication policies, procedures, and controls.
- b) Failing to encrypt personally identifying information in transit and at rest.
- c) Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII.
- d) Failing to adequately monitor the security of their networks and systems.
- e) Allowing unauthorized access to PII and educational records.
- f) Failing to detect in a timely manner that PII had been compromised.
- g) Failing to delete student PII it was no longer required to retain.
- h) Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.
- i) Failing to implement data security practices consistent with Defendant's published privacy policies.

49. Plaintiff and Class Members were within the class of persons the FERPA was intended to protect and the type of unauthorized disclosure that resulted from the Data Breach was the type of harm the statute was intended to guard against.

50. The injuries resulting to Plaintiff and the Classes because of Defendant's failure to use adequate security measures was reasonably foreseeable.

51. Plaintiff and the Classes were the foreseeable victims of a data breach. Defendant knew or should have known of the inherent risks in collecting and storing PII, the critical importance of protecting that PII, and the necessity of password policies and user authentication methods to prevent credential abuse.

52. Plaintiff and the Classes had no ability to protect the PII in Defendant's possession. Defendant was in the best position to protect against the harms suffered by Plaintiff and the Classes as a result of the Data Breach.

53. But for Defendant's breach of duties owed to Plaintiff and the Classes, their PII would not have been compromised. There is a close causal connection between Defendant's failure

1 to implement reasonable security measures to protect the PII of Plaintiff and the Classes and the
2 harm, or risk of imminent harm, suffered by Plaintiff and the Classes.

3 54. As a result of the Data Breach, Plaintiff and Class Members suffered injuries
4 including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost time and
5 opportunity costs associated with attempting to mitigate the actual consequences of the Data
6 Breach; (iv) lost benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or
7 emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk
8 their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized
9 third parties to access; and (b) remains backed up under Defendant's possession or control and is
10 subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and
11 reasonable measures to protect the PII.
12

13 55. Plaintiff and Class Members are entitled to compensatory and consequential
14 damages suffered as a result of the Data Breach.
15

16 56. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant
17 to: (i) strengthen its data protection procedures; and (ii) to provide adequate protection services to
18 all affected by the Data Breach.
19

20 **COUNT 2: BREACH OF IMPLIED CONTRACT**

21 57. Plaintiff re-alleges and incorporates by reference all the allegations contained in the
22 foregoing paragraphs as if fully set forth herein.

23 58. Defendant collects and receives various educational records and other PII, regarding
24 students, teachers, parents and guardians, including Plaintiff and Class Members, in the ordinary
25 course of providing education related products or services.
26
27
28

1 59. Defendant published its privacy principles and privacy statement to inform the
2 public about how Defendant collects, uses, shares, and protects the information Defendant gathers
3 in connection with the provision of those products or services.

4 60. Defendant’s “Privacy Principles” provide, in relevant part, “We seek to protect our
5 customers’ personal data from unauthorized access, use, modification, disclosure, loss, or theft by
6 leveraging various reasonable security measures and methods to secure our customers’ personal
7 data throughout its processing lifecycle with PowerSchool applications. Our overall aim is to ensure
8 the confidentiality, integrity, and availability of our customers’ personal data”

9 61. In so doing, Plaintiff and Class Members entered implied contracts with Defendant
10 by which Defendant agreed to use reasonable technical, administrative, and physical safeguards to
11 “preserve the confidentiality, integrity, and availability of [the] personal information” it collects
12 and stores.

13 62. Plaintiff and Class Members had no meaningful decision or choice regarding the
14 disclosure of the PII to Defendant because the data was collected as part of their educational
15 institution’s use of PowerSchool SIS. Such disclosure to Defendant would not have occurred in
16 the absence of an expressed or implied promise to implement reasonable data protection measures
17 to safeguard the data.

18 63. Plaintiff and Class Members fully and adequately performed their obligations under
19 the implied contract with Defendant.

20 64. Defendant breached the implied contract with Plaintiff and Class Members which
21 arose from the course of conduct between the parties, as well as disclosures on the Defendant’s web
22 site, privacy policy, its contract with each educational institution, and in other documents, all of
23 which created a reasonable expectation that the personal information Defendant collected would be
24

adequately protected and that the Defendant would take such actions as were necessary to prevent unauthorized access to, use of, or disclosure of such information.

65. As a result of the Data Breach, Plaintiff and Class Members suffered injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) lost benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and increased risk their PII will be misused, where: (a) their data remains unencrypted and available for unauthorized third parties to access; and (b) remains backed up under Defendant's possession or control and is subject to further unauthorized disclosures so long as Defendant fails to implement appropriate and reasonable measures to protect the PII.

66. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

67. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its data protection procedures; and (ii) to provide adequate protection services to all affected by the Data Breach.

COUNT 3: UNJUST ENRICHMENT

68. Plaintiff re-alleges and incorporates by reference all the allegations contained in the foregoing paragraphs as if fully set forth herein.

69. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

70. By providing their PII to Defendant at various events, conferences, webinars, or by visiting Defendant's website(s) or by using Defendant's products, Plaintiff and Class Members conferred a monetary benefit on Defendant. Defendant used the PII to market, advertise, and sell

1 additional services to Plaintiff and Class Members. Defendant knew that Plaintiff and Class
2 Members conferred a benefit upon them and have accepted and retained that benefit.

3 71. By collecting the PII, Defendant was obligated to safeguard and protect such
4 information, to keep such information confidential, and to timely and accurately notify Plaintiff
5 and Class Members if their data had been compromised or stolen.
6

7 72. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, it
8 would be unjust for Defendant to retain any of the benefits that Plaintiff and Class Members
9 conferred upon Defendant without paying value in return.

10 73. As a direct and proximate result of the Defendant's conduct, Plaintiff and Class
11 Members suffered injuries. As such, Plaintiff and Class Members are entitled to full refunds,
12 restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits,
13 benefits, and other compensation obtained by Defendant from its wrongful conduct.
14

15 **COUNT 4: INVASION OF PRIVACY**

16 74. Plaintiff re-alleges and incorporates by reference all the allegations contained in the
17 foregoing paragraphs as if fully set forth herein.
18

19 75. Plaintiff and Class Members had a legitimate expectation of privacy in their
20 personally identifying information such as Social Security numbers, medical information, and
21 academic information. Plaintiff and Class Members were entitled to the protection of this
22 information from disclosure to unauthorized third parties.

23 76. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.
24 Yet, Defendant permitted the public disclosure of Plaintiff's and Class Members' PII to
25 unauthorized third parties.
26
27
28

1 77. The PII that was disclosed without the Plaintiff's and Class Members' authorization
2 was highly sensitive, private, and confidential. The public disclosure of the type of PII at issue here
3 would be highly offensive to a reasonable person of ordinary sensibilities.

4 78. Defendant permitted its information technology environment to remain vulnerable
5 to foreseeable threats, which created an atmosphere for the Data Breach to occur. Despite
6 knowledge of the substantial risk of harm created by these conditions, Defendant intentionally
7 disregarded the risk, thus permitting the Data Breach to occur.

8 79. By permitting the unauthorized disclosure, Defendant acted with reckless disregard
9 for the Plaintiff's and Class Members' privacy, and with knowledge that such disclosure would be
10 highly offensive to a reasonable person. Furthermore, the disclosure of the PII at issue was not
11 newsworthy or of any service to the public interest.

12 80. Defendant was aware of the potential of a data breach and failed to adequately
13 safeguard its systems and/or implement appropriate policies and procedures to prevent the
14 unauthorized disclosure of Plaintiff's and Class Members' data.

15 81. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class
16 Members' PII to rise to the level of intentionally allowing the intrusion upon the seclusion, private
17 affairs, or concerns of Plaintiff and Class Members.

18 82. Plaintiff and Class Members have been damaged by the invasion of their privacy in
19 an amount to be determined at trial.

20 **Count 5: VIOLATION OF THE UNFAIR COMPETITION LAW**

21 83. Plaintiff re-alleges and incorporates by reference all the allegations contained in the
22 foregoing paragraphs as if fully set forth herein.

23 84. Defendant engaged in unlawful, unfair, or fraudulent acts and practices and unfair,
24 deceptive, untrue, or misleading acts prohibited by the Business and Professions Code, which
25
26
27
28

1 constitute unfair competition within the meaning of Section 17200 of the Business and Professions
2 Code.

3 85. Defendant's acts or practices that violate Section 17200 include, but are not limited
4 to: (i) failing to implement and maintain reasonable security procedures and practices to protect PII
5 from unauthorized disclosures; (ii) making false, deceptive, or misleading statements regarding its
6 security measures and practices in effect at the time of the Data Breach; and (iii) making or
7 disseminating false or misleading statements with the intent to induce the public to use Defendant's
8 services or products when Defendant knew, or should have known, that its statements were false
9 or misleading.
10

11 86. Plaintiff alleges that Defendant's data security measures remain inadequate.
12 Plaintiff will continue to suffer injury as a result of the compromise of their PII and remain at
13 imminent risk that further compromises of their PII will occur in the future.
14

15 87. Plaintiff and Class Members have suffered irreparable injury, and will continue to
16 suffer injury in the future, as a result of Defendant's deceptive trade practices, which places
17 Plaintiff and Class Members at imminent risk that further compromises of their PII will occur in
18 the future. As such, the remedies available at law are inadequate to compensate for that injury.
19 Accordingly, Plaintiff and Class Members also seek to obtain a judgment declaring, among other
20 things, the following:
21

- 22 a. Defendant continues to owe a legal duty to secure PII and to timely notify
23 consumers of a data breach.
- 24 b. Defendant continues to breach this legal duty by failing to employ reasonable
25 measures to secure Plaintiff and Class Members' PII.

26 88. The Court also should issue corresponding prospective injunctive relief requiring
27 that Defendant employs adequate data protection practices consistent with law and industry
28 standards.

1 89. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to
2 Defendant if an injunction is issued. Among other things, if another massive data breach occurs,
3 Plaintiff will likely be subjected to fraud, identity theft, and other harms described herein. On the
4 other hand, the cost to Defendant of complying with an injunction by employing reasonable
5 prospective data security measures is relatively minimal, and Defendant has a pre-existing legal
6 obligation to employ such measures.
7

8 90. The issuance of the requested injunction will not do a disservice to the public
9 interest. To the contrary, such an injunction would benefit the public by encouraging Defendant
10 to take necessary action to prevent another data breach, thus eliminating the additional injuries
11 that would result to Plaintiff and the multitude of individuals whose PII would be at risk of future
12 unauthorized disclosures.
13

14 91. As a result of the Defendant's false, misleading, or deceptive acts, regarding its
15 data security practices, the consuming public in general, Plaintiff, and Class Members suffered
16 injuries including, but not limited to, the future and continued risk their PII will be misused,
17 where: (a) their data remains unencrypted and available for unauthorized third parties to access;
18 and (b) remains under Defendant's possession or control and is subject to further unauthorized
19 disclosures so long as Defendant fails to implement appropriate and reasonable measures to
20 protect the PII.
21

22 92. Plaintiff and Class Members are entitled to attorneys' fees, costs, and injunctive
23 relief requiring Defendant to: (i) strengthen its data protection procedures; (ii) implement strong
24 authentication mechanisms for accessing cloud services; and (iii) to provide adequate dark web
25 monitoring and/or credit monitoring to all affected by the Data Breach.
26

27 **PRAYER FOR RELIEF**

28 **WHEREFORE**, Plaintiff, individually and on behalf of the other members of the Classes

alleged herein, respectfully requests that the Court enter judgment as follows:

- A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff(s) as the representatives for the Classes and counsel for Plaintiff(s) as Class Counsel;
- B. For an order declaring the Defendant's conduct violates the statutes and causes of action referenced herein;
- C. For an order finding in favor of Plaintiff and the Classes on all counts asserted herein;
- D. Ordering Defendant to pay for lifetime credit monitoring and dark web scanning services for Plaintiff and the Classes;
- E. For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;
- F. For prejudgment interest on all amounts awarded;
- G. For an order of restitution and all other forms of equitable monetary relief requiring the disgorgement of the revenues wrongfully retained as a result of the Defendant's conduct;
- H. For injunctive relief as pleaded or as the Court may deem proper; and
- I. For an order awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses and costs of suit, and any other expense, including expert witness fees; and
- J. Such other relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all claims in this Complaint and of all issues in this action so triable as of right.

Dated: January 10, 2025.

Respectfully submitted,

By: /s/ John C. Bohren
John C. Bohren (California Bar No. 295292)
YANNI LAW APC
P.O. Box 12174
San Diego, CA 92112
Telephone: (619) 433-2803
Fax: (800) 867-6779
yanni@bohrenlaw.com
-AND-

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Paul J. Doolittle (*Pro Hac Vice* Forthcoming)
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com